INSTITUTE FOR DEFENSE ANALYSES

Cyber Insurance – Managing Cyber Risk

Laura A. Odell, *Project Leader*

J. Corbin Fauntleroy

Ryan R. Wagner

April 2015

Approved for public release; distribution is unlimited.

IDA Non-Standard
NS D-5481
Log: H 15-000375
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task BC-5-3897, "Trusted Systems and Networks Analytic Support, and IT Innovation Evaluations," for Department of Defense, Chief Information Officer

The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

B. David Mussington and J. Katharine Burton

Copyright Notice

© 2015 Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [Jun 2013].

IDA Cyber Insurance – Managing Cyber Risk

Data breaches involving significant personal information losses and financial impact are becoming increasingly common. Whether the data breach has financial implications for customers or business partners or results in the loss of private information, companies are being held liable for these losses. The costs can run into the hundreds of millions of dollars depending on the type and size of the breach. Most states have some type of data breach law requiring notification of affected residents within a reasonable timeframe, breaches are being made public much sooner, and business reputations are being affected. As a result, the insurance industry is seeing a sharp increase in demand for cyber insurance offerings to businesses.

What is cyber insurance? Cyber insurance is a risk transfer product that corporations can buy to mitigate losses due to information technology (IT) problems. Gartner has defined cyber insurance as "protection against losses related to cyber risks, such as data theft/loss, business interruption caused by a computer malfunction or virus, and fines or lost income because of system downtime, network intrusion and/or information security breaches."[1] The cyber insurance market, spurred by increasing costs due to loss of personal information, is estimated to be $2 billion and growing.[2]

Who sells it and what does it cover? Major insurance companies like Zurich, American International Group, Inc. (AIG), and Allianz sell cyber insurance products to businesses. In a recent report, Gartner stated that at least 20 insurers sell cyber insurance. Insurance breaks down into two main types: first-party and third-party coverage. First-party policies cover losses incurred directly, like lost income and IT expenses; third-party policies cover liabilities of others, such as damage to others' IT systems and fines for loss of personally identifiable information (PII).[3,4] One Lloyd's of London insurer has created a policy for insuring data stored in the cloud.[5] Typically, businesses that install or service software or networks or provide IT consulting for their clients use third-party insurance. If a breach occurs, it is the people and businesses that developed, maintained, and managed the system that are primarily responsible for data loss. However, non-IT businesses that use an IT system are covered by first-party insurance. For example, Sony incurred substantial first-party losses, including cost for investigation of the system, injury to reputation, and business interruption losses.

Most cyber liability insurance, both first- and third-party, is a combination of four components: errors and omissions, media liability, network security, and privacy. *Errors and omissions* covers claims related to performance of services such as software development or consulting services associated with IT systems. *Media liability* covers claims related to intellectual property or copyright/trademark infringement, libel, and slander. Technology

companies that maintain online content include a media liability component in their coverage. *Network security* covers a failure in network security, which can result in data breaches, destruction of data, virus transmission, and cyber extortion. The *privacy* component covers loss of personal information, including physical records, loss of a laptop with personal information on it, sending a file containing customer data to the wrong email address, or returning leased equipment without wiping the hard drive.[6]

Cyber Insurance Components					
Errors & Omissions	Media	Network Security		Privacy	
Third-party	Third-party	First-party	Third-party	First-party	Third-party
• Negligence or Errors in Product or Performance of Services (includes breach of customer's data) • Failure to perform	• Infringement of Intellectual Property (other than patent) • Advertising & Personal Injury	• Unauthorized Access • Transmission of Virus or Malicious Code • Theft/Destruction of Data • Cyber Extortion • Business Interruption		PII/PHI Data Exposed by: • Hacker • Lost Device • Rogue Employee • Physical Records	

Source: Woodruff-Sawyer and Company, http://www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-basics

If a data breach occurs, first-party insurance most commonly covers notifying clients that their information was compromised or exposed, credit monitoring services for customers affected by the breach, public relations campaigns to restore the reputation of the business, compensation for income that the business was not able to earn while it recovered from the breach, expenses related to regulatory compliance, and payment to a cyber-extortionist holding data hostage or threatening an attack. Third-party coverage shields a business when its clients suffer a breach because of an alleged mistake on the business's part and covers settlements or judgments and any court costs that result from a data breach.

Why are people buying it? According to insurance underwriters and brokers, two of the main reasons businesses purchase cyber insurance are: (1) the increasingly ominous stories of major breaches and (2) new requirements that mandate cyber coverage.[7]

Whereas previously a customer might not ever have known that his or her data had been compromised, 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands now have laws requiring private or government entities to notify affected individuals of security breaches involving PII in a timely manner.[8] The laws identify the type of information that should be reported and the timeframe within which notification should occur. There are also federal regulations with respect to data breaches. The Health Insurance Portability and Accountability Act (HIPPA) Breach Notification Rule 45 CFR §§ 164.400-414 contains guidelines for notifying consumers when their private health information has been breached. The Federal Trade Commission has been promoting a federal data breach law to standardize the rules for notification and penalties for data breaches. As federal and state governments impose financial penalties for the loss of PII, cyber insurance is likely to become a more critical risk-management tool.

What are the drawbacks? One insurance executive stated that cyber insurance "is a difficult risk to price by traditional insurance methods as there currently is not statistically significant actuarial data available."[9] This has led to steeply rising prices for these insurance products. Insurance lawyer David E. Wood suggests that cyber insurers are underpricing their products and are not prepared for a catastrophic cyber event.[10] Stephen Catlin, CEO of a Lloyd's of London insurer, stated that cyber risk is the "biggest, most systemic risk" he has seen in his career.[11] Other researchers also note a number of problems with cyber insurance, including unclear coverage, the lack of good actuarial data, and the "lack of adequate reinsurance" for cyber insurers.[12,13,14]

Crucially for the Department of Defense (DoD), many cyber insurance policies exempt from coverage the types of scenarios most likely to affect the department. A cyber insurance policy from AIG specifically excludes Acts of War, including "…military action (whether war is declared or not)…," and Government Action "arising out of, based upon or attributable to any seizure, confiscation, nationalization, breach of security, use, misuse or destruction of a Computer System or Electronic Data by or on behalf of any governmental, military, enforcement or other public body or authority…."[15]

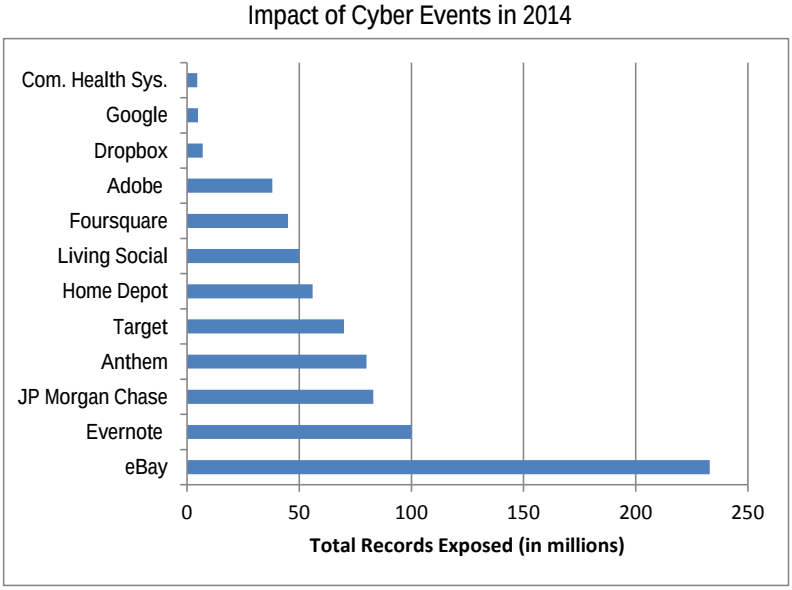
The cyber insurance policy from Allianz similarly excludes "War, Terrorism, looting and Governmental Acts."[16] "War means war, any invasion, act of foreign enemy, hostile operations (whether war has been declared or not)…." Additionally, both the AIG and Allianz policies exclude losses of trade secrets and intellectual property. AIG even excludes the loss of personal information from coverage.

Even in the cases in which cyber insurance does cover a loss, it may not cover 100 percent of the damages. Cyber insurance covered only half of the costs associated with the Home Depot and Target breaches.[2]

What role does cyber insurance play in cybersecurity? To understand how cyber insurance can improve security for businesses, it is important to understand the role insurance plays in managing risk. Insurance is designed to cover loss due to unforeseen circumstances. Coverage and premiums are based on the probability of the event happening and the expected financial loss. Thus, insurance allows businesses to transfer and pool their risk, thereby reducing the financial impact if an unforeseen event occurs.

Insurance has played a key role in the development of modern safety codes and standards in a number of industries. One example is the fire suppression sprinkler systems that we have today. When sprinklers were originally developed in the late 1800s, they were shown to be effective in reducing the damage caused by fires. But standards for pipe size and sprinkler placement varied widely, resulting in some unreliable systems (i.e., small pipes, less water flow; too-wide placement, less coverage). In 1895, representatives of the sprinkler and fire insurance industries had a series of meetings to discuss the issue. These

meeting resulted in standards for sprinkler installation that were implemented by the sprinkler industry and required by insurance underwriters.[17]



Adapted from: Cyber Risk Network

A similar situation exists today; every year, more and more businesses are experiencing cyber attacks resulting in significant loss of data. At the same time, there is little standardization of the processes for managing cyber risk. Insurers can play a key role in creating standardized cyber risk-management processes that will reduce the probability of a successful attack and bolster a business's security posture. Similar to the fire protection industry, insurers can promote information sharing among businesses to identify new threats and vulnerabilities and how to protect from them.

The U.S. Department of Homeland Security (DHS) states that "A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection."[18] According to the Department of the Treasury, "Cyber insurance could cause critical infrastructure policyholders to bolster cybersecurity since insurers have strong financial incentives to establish minimum-security standards, monitor cyber threats, and improve the quality of data collection."[19]

Insurance companies face many challenges in developing cybersecurity insurance policies due to a lack of data that can be used to develop actuarial tables, upon which insurance coverage and premiums are based. Insurers writing cyber policy coverage are interested in the risk-management approach a business applies to protect its networks and its assets and thereby lessen the impact of an attack. This includes disaster response plans, how employees and others access data systems, and at a minimum, the antivirus and anti-malware software used by the business, the frequency of updates, and the performance of firewalls.

What role does the U.S. Government play in cyber insurance? The Federal Government has a vested interest in protecting national security assets, such as critical cyber infrastructure and sensitive data. An evolving cyber insurance market currently relies on policies that can have significant cost and limited coverage. In the face of these restrictions, the private sector has encouraged Congress to develop legislation or extend existing legislation that provides liability protections for the providers of cyber security solutions or participants in information sharing programs in the event of a cyber attack. For example, the 113th Congress entertained expanding the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) to qualified cyber incidents.

The purpose of the SAFETY Act was and is to incentivize the sellers of anti-terrorism technologies who might not bring needed techniques to market because of fear of liability and unaffordability of insurance for third-party claims arising from an act of terrorism. Expansion of the existing SAFETY Act or creation of additional, similar legislation for cyber security technologies could be a statutory method of limiting liability, with the intent to allow for affordable cyber insurance policies. Although the SAFETY Act does not preclude providers of cyber security technologies from obtaining protections, the application of the statute is limited to acts of terrorism, which may not include all cyber events.

Aside from legislation, it is not clear what the U.S. Government's role in cyber insurance should be. However, one role might be promoting collaboration and cooperation across private industry and government to facilitate information sharing, allowing IT security professionals to reduce known vulnerabilities across their systems. Information sharing is an important component of cyber risk management and a requirement for many cyber insurance programs.

One method for public–private collaboration currently in place is the information sharing and analysis centers (ISAC), created in 1998 by presidential directive. The ISACs act as neutral parties that work within sectors to address physical and cyber threats, incidents, and vulnerabilities.[20] Covering a wide range of sectors, including defense, electrical services, health care, and IT, the ISACs provide information on current threats, vulnerabilities, and incidents for dissemination to all ISAC members. However, the promise of the ISACs has never been fully realized. American Express (AmEX) Chairman and CEO, Kenneth Chenault recently said that AmEX "sources over 100,000 attack indicators yearly from various sources, but only five percent come from industry sharing through their ISAC and less than one percent comes from the government."[21] National policy has shifted the model for information sharing to one focusing on standards-based sharing in certified "information sharing and analysis organizations (ISAOs)." Where the ISACs are sector-based, the ISAOs are affinity-based and focus on particular emerging threats and

Anthem – A Case Study

On January 29, 2015, Anthem, Inc., learned of a breach to its IT systems. The breach resulted in the loss of private information about current and former Anthem members. Upon learning of incident, the company began working to close the vulnerabilities and contacted the FBI to begin an investigation. Anthem contacted its members about 2 weeks later.[25] Investigators suspect state-sponsored Chinese hackers are linked to the attack. Attackers leveraged a vulnerability in the encryption of PII data; data was encrypted in transit but not on its servers, which is where the attack occurred.

Approximately 80 million records were accessed containing names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and employment information, including income data. Anthem does not believe credit card or banking information was compromised, nor was there evidence that medical information was obtained.[25]

While the eventual costs are currently unknown, they will include the cost of identity protection services for affected customers and of fines and lawsuits (over 50 at this time). It has been reported that Anthem has $10 million in primary cyber coverage and has $150 million to $200 million in cyber coverage from an American International Group (AIG), Inc., unit and additional insurance through other providers, although it is unlikely that the insurance will cover the majority of the costs.[26]

vulnerabilities. ISAO membership can cross sectors, regions, and other similar interests.[22,23]

Another potential role for government would be fostering the development of exposure models for cyber risk based on the experience of the Defense Industrial Base (DIB) – where it should have the most serial and complete data sets. Even if the data quality is high, however, questions would remain on the broad applicability of defense sector cyber risk numbers, given the special (e.g., state sponsorship) nature of most of the purported attackers.

What does this mean for DoD? DoD is not the intended customer for cyber insurance, but many of the risk-management elements required by insurers would be useful in maintaining cybersecurity. DoD already promotes the use of best practices to limit the probability that losses of sensitive information will occur. It currently requires contractors to have IT risk-management plans, which aligns with the idea that a risk-management plan should be in place before a business can be insured. In addition, DoD requires contractors to report evidence of a cyber attack within 72 hours of the event. Several Defense Federal Acquisition Regulation Supplements (DFARS) have been created over the past few years to address cybersecurity for IT systems developed for DoD.

Some within the DoD have suggested that it should require all defense contractors that store and process sensitive information to obtain cyber insurance. They feel that the requirements in the DFAR promote checklist compliance and that companies will be incentivized to put in place and actively manage cybersecurity and risk management procedures in order to become and stay insured.

However, major exclusions (such as acts of war or government actions) in current insurance policies severely limit their usefulness for DoD. These exclusions are the very things from which DoD is interested in protecting its data and IT resources. Cyber insurance is more focused on protecting data and systems from criminal activity; it is not clear what additional cybersecurity protection might be needed against cyber industrial espionage or to protect our critical infrastructure from terrorist attack. In addition, federal and state data breach laws already encourage companies that store and process PII data for DoD to obtain cyber insurance.

This gap between insurable losses from cyber operations by non-state and non-state-affiliated actors attacking critical infrastructures (including the DIB entities) and non-insurable losses suffered from attacks by foreign-state-affiliated groups or proxies needs to be addressed. Privately provided insurance coverage is unlikely to provide protection in these situations absent some form of government subsidy.

A common suggestion is to establish a government-sponsored enterprise (GSE) or other mechanism to back any major losses due to acts of war, government actions, or terrorist attacks. It has been suggested that these types of attacks would be considered catastrophic and thus should be supported by the government (e.g., federal disaster relief). But federal backing of catastrophic events assumes that significant cyber attacks would be infrequent, and it is clear that with the number of attacks increasing each year, this assumption is incorrect.

Also, GSE backing could create a situation of moral hazard, in which insurers and reinsurers deliberately prepare themselves for small losses (through increased profit-taking and/or lower premiums) while passing the bill for large losses to the government via the GSE. This could result in significant financial impact on the government. The top 14 cyber events in 2014 had a total estimated cost of over $250 million, and that cost is expected to be much greater in 2015.[24] As the frequency of cyber attacks increases, it is likely that costs for a GSE could quickly rise.

As the market matures, insurers are likely to set premiums in a way that encourages effective risk management. This could drive defense contractors to improve cybersecurity preparedness in ways that make a difference. Additionally, cyber insurance could still cover non-governmental actions, such as criminal theft of DoD PII. While cyber insurance is no panacea for DoD, it can push defense contractors to improve cybersecurity while providing limited coverage of some cyber losses.

References

[1] Gartner, “Five Tips for Companies Considering Cyber Insurance,” 2 March 2015. Available: http://blogs.gartner.com/john-wheeler/five-tips-for-companies-considering-cyber-insurance/ [Accessed 31 March 2015].

[2] V. Basani, "Opinion: Cybersecurity insurance – weighing the costs and the risks," MarketWatch.com, 25 March 2015. Available: http://www.marketwatch.com/story/cybersecurity-insurance-weighing-the-costs-and-the-risks-2015-03-25 [Accessed 31 March 2015].

[3] AON, "Cyber Risk Solutions," AON.com. Available: www.aon.com/attachments/risk-services/cyber/Aon-Cyber-Risk-Solutions-General.pdf [Accessed 31 March 2015].

[4] Gartner, "Understanding When and How to Use Cyber Insurance Effectively," 26 April 2012. Available: www.gartner.com/document/1997318 [Accessed 31 March 2015].

[5] CFC Underwriting Ltd. "Lloyd's MGA CFC Underwriting announces today the launch of a new cyber liability wording to cover the risks of storing data 'in the cloud'," 13 December 2011. Available: www.cfcunderwriting.com/media/press-releases/13-12-2011.aspx [Accessed 31 March 2015].

[6] L. Floresca, Cyber Insurance 101: The Basics of Cyber Coverage, WSandCo.com. Available: www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-basics [Accessed 31 March 2015].

[7] Advisen, "Cyber Liability Insurance Market Trends: Survey," October 2014. Available: www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf [Accessed 31 March 2015].

[8] National Conference of State Legislatures, "Security Breach Notification Laws," NCLS.org. Available : www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [Accessed 17 April 2015].

[9] L. Thomas and J. Finkle, "Insurers struggle to get grip on burgeoning cyber risk market," Reuters.com, 14 July 2014. Available: www.reuters.com/article/2014/07/14/us-insurance-cybersecurity-idUSKBN0FJ0B820140714. [Accessed 31 March 2015].

[10] D. E. Wood, "Are Insurers Underestimating the Cyberthreat?," RMMagazine.com, 2 March 2015. Available: www.rmmagazine.com/2015/03/02/are-insurers-underestimating-the-cyberthreat/. [Accessed 31 March 2015].

[11] A Gray, "Government resists calls to fund backstop for cyber disaster losses," FT.com, Available: www.ft.com/cms/s/0/7f9d8326-d096-11e4-a840-2 [Accessed 31 March 2015].

[12] C. Biener, M. Eling and J. H. Wirfs, "Insurability of Cyber Risk: An Empirical Analysis," The Geneva Papers, vol. 40, pp. 131-158, 2015.

[13] D. K. Moulinos, "Incentives and barriers for the cyber insurance market in Europe," Enisa.Europa.com. Available: www.enisa.europa.eu/media/news-items/cyberinsurance_final.pdf. [Accessed 31 March 2015].

[14] N. Robinson, "Incentives and barriers of the cyber insurance market in Europe," 28 June 2012. Available: www.enisa.europa.eu/activities/Resilience-and-CIIP/national-

cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe. [Accessed 31 March 2015].

[15] American International Group, Inc., "CyberEdge PC," AIG.com. Available: www.aig.com/Chartis/internet/US/en/CyberEdge%20PC%20Policy%20Final%202014_tcm3171-595897.pdf [Accessed 31 March 2015].

[16] Allianz, "Allianz Cyber Protect: Digital Business Protection Insurance," AGSC-Cyber-Protect.co.uk, Available: agcs-cyber-protect.co.uk/downloads/agcs_cyberprotect_wording.pdf [Accessed 31 March 2015].

[17] National Fire Protection Association, History of NFPA, NFPA.org : www.nfpa.org/about-nfpa/nfpa-overview/history-of-nfpa [Accessed 30 March 2015].

[18] Department of Homeland Security, "Cyber Security Insurance," DHS.gov. Available: www.dhs.gov/publication/cybersecurity-insurance. [Accessed 30 March 2015].

[19] Department of the Treasury, "Cybersecurity Incentives Pursuant to Executive Order 13636."

[20] National Council of Information Sharing and Analysis. Centers, "National Council of ISACs," ISACCouncil.org. Available: www.isaccouncil.org/home.html. [Accessed 31 March 2015].

[21] R. King, "Obama Signs Info Sharing Executive Order, But Concerns Remain," Blogs.WSJ.com, February 13, 2015. Available: blogs.wsj.com/cio/2015/02/13/obama-signs-info-sharing-executive-order-but-concerns-remain/ [Accessed April 16, 2015].

[22] Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing, February 13 2015. Available: http://www.gpo.gov/fdsys/pkg/DCPD-201500098/pdf/DCPD-201500098.pdf [Accessed April 16 2015].

[23] Department of Homeland Security, "Frequently Asked Questions About Information Sharing and Analysis Organizations," DHS.gov. Available: www.dhs.gov/isao-faq [Accessed April 16, 2015].

[24] J. Bradford, "2014 by the numbers: record setting cyber breaches," CyberRiskNetwork.com, 31 December 2014. Available: www.cyberrisknetwork.com/2014/12/31/2014-year-cyber-breaches/ [Accessed 31 March 2015].

[25] Anthem, "How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services," AnthemFacts.com. Available: www.anthemfacts.com [Accessed 31 March 2015].

[26] D. Walker, "Report: Anthem may have up to $200M in cyber insurance," SCMagazine.com,10 February 2015. Available: www.scmagazine.com/report-anthem-may-have-up-to-200m-in-cyber-insurance/article/397460/ [Accessed 31 March 2015].

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number**. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-04-15	Non-Standard - Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Insurance – Managing Cyber Risk	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
J. Corbin Fauntleroy Ryan R. Wagner Laura A. Odell	BC-5-3897
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-5481 H 15-000375

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
John R. Mills Chief, Cybersecurity Strategy Division Office of the Deputy CIO for Cybersecurity Department of Defense 6000 Defense Pentagon, 3D1048, Washington, D.C. 20301-6000	DoD CIO
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Laura A. Odell

14. ABSTRACT

This paper provides an overview of the components of cyber insurance, discusses the role of the government, and examines specific implications to the Department of Defense. Data breaches involving significant personal information losses and financial impacts are becoming increasingly common. Increasingly, companies are being held liable for these losses, which have financial implications for customers and business partners or result in the loss of private information. Claims of hundreds of millions of dollars are being amassed depending on the type and size of the breach. As a result, the insurance industry is experiencing a sharp increase in demand for cyber insurance offerings to businesses.

15. SUBJECT TERMS

Cybersecurity, Cyber Insurance, Risk Profiles

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			John R. Mills
Unclassified	Unclassified	Unclassified	Unlimited	14	19b. TELEPHONE NUMBER (Include Area Code) 703-695-0906